**15.26 Computer Fraud—Use of Protected Computer**

**(18 U.S.C. § 1030(a)(4))**

The defendant is charged in [Count \_\_\_\_\_\_\_ of] the indictment with computer fraud in violation of Section 1030(a)(4) of Title 18 of the United States Code. For the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly [accessed without authorization] [exceeded authorized access to] a computer [that was exclusively for the use of a financial institution or the United States government] [that was not exclusively for the use of a financial institution or the United States government, but the defendant’s access affected the computer’s use by or for the financial institution or the United States government] [used in or affecting interstate or foreign commerce or communication] [located outside the United States but using it in a manner that affected interstate or foreign commerce or communication of the United States];

Second, the defendant did so with the intent to defraud;

Third, by [accessing the computer without authorization] [exceeding authorized access to the computer], the defendant furthered the intended fraud; [and]

Fourth, the defendant by [accessing the computer without authorization] [exceeding authorized access to the computer] obtained anything of value[.] [; and]

[Fifth, the total value of the defendant’s computer use exceeded $5,000 during [*specify applicable period*.]]

**Comment**

As to intent to defraud, *see* Instruction 4.13 (Intent to Defraud).

Use the fifth element of this instruction when the prosecution’s theory is that the object of the defendant’s alleged fraud was only the use of the computer, and the value of that computer use was “more than $5,000 in any 1-year period.” This fifth element reflects the requirements of 18 U.S.C. § 1030(a)(4), which apply where the defendant’s purpose and the thing of value the defendant obtained by the fraud was only the use of the computer.

18 U.S.C. § 1030(e) provides definitions of the terms “computer,” “financial institution,” and “exceeds authorized access.” While the term “protected computer” is defined in 18 U.S.C. § 1030(e), that term is not used in the elements of this instruction because that definition has been incorporated into the first element of the instruction. Accordingly, it is not necessary to provide a separate definition of “protected computer.”

Interpreting the civil counterpart to § 1030 and expressly finding such interpretation equally applicable in the criminal context, the Ninth Circuit held that “a person uses a computer ‘without authorization’ under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone’s computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009). The court further held that an employee’s use of a computer contrary to the employer’s interest does not alone satisfy the “without authorization” prong of the statute. *Id.*

The Ninth Circuit has held that the phrase “exceeds [or exceeded] authorized access” is limited to violations of restrictions on access to information and not restrictions on the use of information that is permissibly accessed. *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012); *see also United States v. Christensen*, 828 F.3d 763, 786-87 (9th Cir. 2015), *as amended on denial of reh’g* (2016).

*Revised June 2019*